UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/293,142	04/16/1999	TAKASHI KONDOH	990242LH	4480

7590 09/16/2004

FRISHAUF HOLTZ GOODMAN
767 THIRD AVENUE 25TH FLOOR
NEW YORK, NY 100172023

EXAMINER	
MOORTHY, ARAVIND K	

ART UNIT	PAPER NUMBER
2131	12

DATE MAILED: 09/16/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/293,142	Applicant(s) KONDOH ET AL.	
	Examiner Aravind K Moorthy	Art Unit 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 March 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) *2,9 and 11-13* is/are withdrawn from consideration.

5)☒ Claim(s) *10,15,17 and 18* is/are allowed.

6)☒ Claim(s) *1,3-8,14,16 and 19-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 April 1999* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-27 are pending.

2. Claims 2, 9 and 11-13 have been cancelled.

3. Claims 1, 3-8, 14, 16 and 19-27 stand being rejected.

4. Claims 10, 15, 17 and 18 are allowed.

Response to Arguments

5. Applicant's arguments with respect to claims 1-18 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1, 3 and 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Friedman U.S. Patent No. 5,499,294 in view of Moghadam et al U.S. Patent No. 5,801,856.

As to claims 1 and 7, Friedman discloses a camera including an image pickup unit for picking up an image of an object [figure 3a]. Friedman discloses an encryption processing unit for generating alteration detection data using a built-in encryption key from the image data picked up by the image pickup unit [figure 3b]. Friedman discloses an alteration detection unit for decrypting the alteration detection data generated by the encryption processing unit using a decryption key corresponding to the encryption key [figure 3c]. Friedman discloses detecting whether the image data has been altered based on a result of the decryption [column 6, lines 30-

52]. Friedman discloses that the encryption processing unit generates the alteration detection data based on the encryption key, the image data, and data for identifying a photographer [column 6, lines 2-29]. Friedman discloses that the encryption processing unit also utilizes data obtained by application of a predetermined function to the image data to generate the alteration detection data [column 7, lines 18-45].

Friedman does not teach means for identifying a photographer that is removably connected to the camera and that it includes data for identifying the photographer. Friedman does not teach that the encryption processing unit generates the alteration detection data using the encryption key from a combination of the image data and the data for identifying the photographer.

Moghadam et al teaches means for identifying a photographer that is removably connected to the camera and that it includes data for identifying the photographer [column 3, lines 24-48]. Moghadam et al teaches that the encryption processing unit generates the alteration detection data using the encryption key from a combination of the image data and the data for identifying the photographer [column 3 line 58 to column 4 line 10].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Friedman so that there would have been means for identifying a photographer that was removably connected to the camera and that it included data for identifying the photographer. The encryption processing unit would have generated the alteration detection data using the encryption key from a combination of the image data and the data for identifying the photographer.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Friedman by the teaching of Moghadam because it provides security of a digital image produced from a photographic image by the photographer at the time that the original photographic image is produced [column 2, lines 11-14].

As to claim 3, Friedman teaches that the alteration detection unit detects whether or not the image data has been altered by comparing the data obtained by application of the predetermined function to the image data with data obtained by decrypting the alteration detection data using the decryption key [column 6, lines 2-29].

7. Claims 4-6, 14, 16 and 19-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Squilla et al U.S. Patent No. 5,898,779 in view of Moghadam et al U.S. Patent No. 5,801,856.

As to claims 4-6, 14 and 16, Squilla et al discloses a camera including an image pickup unit for picking up an image of an object [figure 2]. Squilla et al discloses encryption processing unit for generating alteration detection data using a built-in encryption key from the image data picked up by the image pickup unit [figure 2]. Squilla et al discloses an alteration detection unit for decrypting the alteration detection data generated by the encryption processing unit using a decryption key corresponding to the encryption key [figure 6]. Squilla et al discloses detecting whether the image data has been altered based on a result of the decryption [figure 6]. Squilla et al discloses that the encryption processing unit generates the alteration detection data based on the encryption key, the image data, and data for identifying a photographer [figure 5]. Squilla et al discloses that the encryption processing unit generates first data from the image data using the encryption key, generates second data from the image data using the data for identifying the

photographer, and combines the first data and the second data into the alteration detection data [figure 5]. Squilla et al suggests that the second encryption processing unit is removably mounted on the camera [figure 2]. Squilla et al discloses that the image data comprises multiple resolution image data including a plurality of image data of different resolutions combined and stored in different sets [column 8 line 52 to column 9 lines 15]. Squilla et al discloses that the encryption processing unit includes a selection unit for selecting at least one image data having a desired resolution from the multiple resolution image data in order to generate the alteration detection data [column 8 line 52 to column 9 lines 15]. Squilla et al discloses that the image data comprises multiple resolution image data including a plurality of image data of different resolutions combined and stored in different sets [column 8 line 52 to column 9 lines 15]. Squilla et al discloses that each of the multiple resolution image data is stored in units of a predetermined small block [column 8 line 52 to column 9 lines 15]. Squilla et al discloses that the encryption processing unit generates the alteration detection data in units of the small block [column 8 line 52 to column 9 lines 15].

Squilla et al does not teach means for identifying a photographer that is removably connected to the camera and that it includes data for identifying the photographer. Squilla et al does not teach that the encryption processing unit generates the alteration detection data using the encryption key from a combination of the image data and the data for identifying the photographer.

Moghadam et al teaches means for identifying a photographer that is removably connected to the camera and that it includes data for identifying the photographer [column 3, lines 24-48]. Moghadam et al teaches that the encryption processing unit generates the alteration

detection data using the encryption key from a combination of the image data and the data for identifying the photographer [column 3 line 58 to column 4 line 10].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Squilla et al so that there would have been means for identifying a photographer that was removably connected to the camera and that it included data for identifying the photographer. The encryption processing unit would have generated the alteration detection data using the encryption key from a combination of the image data and the data for identifying the photographer.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Squilla et al by the teaching of Moghadam because it provides security of a digital image produced from a photographic image by the photographer at the time that the original photographic image is produced [column 2, lines 11-14].

As to claims 19, 21 and 23, Squilla et al teaches that the encryption processing unit also utilizes data obtained by application of a predetermined function to the image data to generate the alteration detection data [figure 5].

As to claims 20, 22 and 24, Squilla et al teaches that the alteration detection unit detects whether or not the image data has been altered by comparing the data obtained by application of the predetermined function to the image data with data obtained by decrypting the alteration detection data using the decryption key [figure 6].

8. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Squilla et al U.S. Patent No. 5,898,779 in view of Steinberg U.S. Patent No. 5,862,218 and Moghadam et al U.S. Patent No. 5,801,856.

As to claim 8, Squilla et al discloses a camera including an image pickup unit for picking up an image of the object. Squilla et al discloses an encryption processing unit for generating alteration detection data using a built-in encryption key from the image data obtained by the image pickup unit. Squilla et al discloses an alteration detection unit for decrypting the alteration detection data generated by the encryption processing unit using a decryption key corresponding to the encryption key. Squilla et al discloses detecting whether the image data has been altered based on a result of the decryption, all discussed above. Squilla et al discloses that the camera includes a mode selection unit for selecting at least one of an alteration monitor mode for detecting whether the image data has been altered. Squilla et al discloses a secure mode for encrypting the image data transferred from the camera to the alteration detection unit, all as discussed above. Squilla et al suggests a normal mode for taking a photograph without a security function [figure 2].

Squilla et al does not teach a digital watermark mode for embedding a digital watermark in the image data. Squilla et al does not teach means for identifying a photographer that is removably connected to the camera and that it includes data for identifying the photographer. Squilla et al does not teach that the encryption processing unit generates the alteration detection data using the encryption key from a combination of the image data and the data for identifying the photographer.

Steinberg teaches a digital camera with a digital watermark mode for embedding a digital watermark in the image data [abstract].

Moghadam et al teaches means for identifying a photographer that is removably connected to the camera and that it includes data for identifying the photographer [column 3,

lines 24-48]. Moghadam et al teaches that the encryption processing unit generates the alteration detection data using the encryption key from a combination of the image data and the data for identifying the photographer [column 3 line 58 to column 4 line 10].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Squilla et al so that one of the modes as taught would have included a digital watermark mode for embedding a digital watermark in the image data. There would have been means for identifying a photographer that was removably connected to the camera and that it included data for identifying the photographer. The encryption processing unit would have generated the alteration detection data using the encryption key from a combination of the image data and the data for identifying the photographer.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Squilla et al by the teaching of Steinberg and Moghadam because it provides a marked, secure images that minimizes concerns regarding unauthorized use [Steinberg column 2 line 15 to column 3 line 3]. It provides security of a digital image produced from a photographic image by the photographer at the time that the original photographic image is produced [Moghadam column 2, lines 11-14].

9. Claims 25-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Squilla et al U.S. Patent No. 5,898,779 in view of Hamada et al U.S. Patent No. 5,185,798 and Moghadam et al U.S. Patent No. 5,801,856.

As to claim 25, Squilla et al discloses a camera including an image pickup unit for picking up an image of an object. Squilla et al discloses a first encryption processing unit for

generating first alteration detection data using a built-in encryption key from the image data picked up by the image pickup unit. Squilla et al discloses an alteration detection unit for decrypting the first alteration detection data generated by the encryption processing unit using a decryption key corresponding to the encryption key. Squilla et al discloses detecting whether the image data has been altered based on a result of the decryption. Squilla et al discloses a storage unit for storing data for identifying a photographer and the encryption key. Squilla et al discloses a second encryption processing unit for generating second alteration detection data from the data for identifying the photographer, all as discussed above.

Squilla et al does not teach that the second encryption processing unit is removably mounted on the camera. Squilla et al does not teach means for identifying a photographer that is removably connected to the camera and that it includes data for identifying the photographer. Squilla et al does not teach that the encryption processing unit generates the alteration detection data using the encryption key from a combination of the image data and the data for identifying the photographer.

Hamada et al teaches an IC card that includes an encrypting circuit [abstract].

Moghadam et al teaches means for identifying a photographer that is removably connected to the camera and that it includes data for identifying the photographer [column 3, lines 24-48]. Moghadam et al teaches that the encryption processing unit generates the alteration detection data using the encryption key from a combination of the image data and the data for identifying the photographer [column 3 line 58 to column 4 line 10].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Squilla et al so that the images would have been

stored on the IC card. The IC card would have been removable from the camera. There would have been means for identifying a photographer that was removably connected to the camera and that it included data for identifying the photographer. The encryption processing unit would have generated the alteration detection data using the encryption key from a combination of the image data and the data for identifying the photographer.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Squilla et al by the teaching of Hamada et al because even if the data is tampered with, identification can be made, upon request by the IC card owner, on the card issuing person's side, whether or not the data in the magnetic or optical recording area is tampered with [column 5, lines 20-25]. It provides security of a digital image produced from a photographic image by the photographer at the time that the original photographic image is produced [Moghadam column 2, lines 11-14].

As to claim 26, the Squilla-Hamada-Moghadam combination teaches that the encryption processing unit utilizes data obtained by application of a predetermined function to the image data to generate the alteration detection data [i.e. hashing function].

As to claim 27, the Squilla-Hamada-Moghadam combination teaches that the alteration detection unit detects whether or not the image data has been altered by comparing the data obtained by application of the predetermined function to the image data with data obtained by decrypting the alteration detection data using the decryption key [Squilla figure 6].

Allowable Subject Matter

10. Claims 10, 15, 17 and 18 are allowed.

As to claim 10, prior art teaches a filing management unit for filing and managing the image data input thereto through an image input unit. Prior art teaches an alteration detection unit for decrypting first alteration detection data attached to the image data by use of a decryption key corresponding to a first encryption key used for generating the alteration detection data. Prior art teaches comparing the first alteration detection data thus decrypted with the image data thereby to detect the alteration of the image data. Prior art teaches an image editing unit for processing the image data and an image file updating unit for generating second alteration detection data, all as discussed above.

Prior art does not teach or fairly discloses using a second encryption key other than the first encryption key from the image data processed by the image editing unit and editing history data output by the image editing unit, and for adding the second alteration detection data to the edited image data. Prior art does not teach or fairly discloses means for adding and storing editor authentication data read from a detachable IC card. Prior art does not teach or fairly discloses that the image file updating unit is removably mounted on the digital image editing system and has stored therein the editor authentication data and the second encryption key. Prior art does not teach or fairly discloses that the second alteration detection data is generated using the second encryption key and the editor authentication data.

Any claim not directly addressed is allowed on the virtue of its dependency.

Conclusion

11. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K Moorthy whose telephone number is 703-305-1373. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Aravind K Moorthy
May 13, 2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100